IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA	)	
	)	DOCKET NO. 3:24-CR-76-KDB
v.	)	
	)	**FACTUAL BASIS**
CHIRAG TOMAR	)	
	)	

NOW COMES the United States of America, by and through Dena J. King, United States Attorney, and hereby files this Factual Basis in support of the plea agreement filed simultaneously in this matter.

This Factual Basis is filed pursuant to Local Criminal Rule 11.2 and does not attempt to set forth all of the facts known to the United States at this time. By their signatures below, the parties expressly agree that there is a factual basis for the guilty plea(s) that the defendant will tender pursuant to the plea agreement, and that the facts set forth in this Factual Basis are sufficient to establish all of the elements of the crime(s). The parties agree not to object to or otherwise contradict the facts set forth in this Factual Basis.

Upon acceptance of the plea, the United States will submit to the Probation Office a "Statement of Relevant Conduct" pursuant to Local Criminal Rule 32.4. The defendant may submit (but is not required to submit) a response to the Government's "Statement of Relevant Conduct" within seven days of its submission. The parties understand and agree that this Factual Basis does not necessarily represent all conduct relevant to sentencing. The parties agree that they have the right to object to facts set forth in the presentence report that are not contained in this Factual Basis. Either party may present to the Court additional relevant facts that do not contradict facts set forth in this Factual Basis.

1. From at least June 2021 until at least August 2022, Chirag TOMAR did knowingly combine, conspire, confederate, and agree with others known and unknown to commit the offense of wire fraud. It was a part of and an object of the conspiracy that TOMAR and others known and unknown, with the intent to defraud, having devised the scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and by concealment of material facts, and for the purpose of executing and attempting to execute such scheme and artifice, transmitted and caused to be transmitted by means of wire communication in interstate commerce, writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code, Section 1343. TOMAR willfully joined and participated in the conspiracy while knowing its unlawful purpose, all in violation of Title 18, United States Code, Section 1349.

2. TOMAR, a citizen and resident of the Republic of India, engaged in a conspiracy to steal cryptocurrency from hundreds of victims through fraud. TOMAR and others stole millions of dollars' worth of various cryptocurrencies from victims worldwide. During the time period of the fraud conspiracy, TOMAR resided in the Republic of India.

3. Beginning as late as June 2021, TOMAR and known and unknown coconspirators stole cryptocurrency in the form of Bitcoin, Ethereum, and Tether from victims throughout the United States and elsewhere through the use of a spoofed Coinbase website. Spoofing, as it pertains to cybersecurity, is when a malicious cyber actor disguises an email address, sender name, or website URL—often just by changing one letter, symbol, or number—to convince a victim that the victim is interacting with a trusted source. Here, the conspirators spoofed the legitimate Coinbase Pro cryptocurrency exchange website through the use of a similar, but unaffiliated, website URL: "CoinbasePro.com."

4. When a victim Coinbase customer would inadvertently visit CoinbasePro.com, he or she would be redirected to one of many websites that were intentionally designed to be similar to the legitimate Coinbase log-in website. Misled by the fraudulently designed websites, victims would then attempt to log in with their valid Coinbase credentials, which resulted in the victims' Coinbase log-in credentials being acquired by the fraudsters. Victims would then be notified that his or her account was locked and prompted to either: (1) call a phone number that was provided in order to speak to a purported Coinbase customer service representative, or (2) use the website's live chat box feature. The phone number connected the victim to a coconspirator who claimed to be an employee of Coinbase. Typically, at this point in the fraud scheme, a real password-reset link would then be sent to the victim and the fraudulent Coinbase representative would request that the victim provide the real password-reset link in the live website chat. The link provided by the victim was a legitimate link from Coinbase allowing the actor to change the victim's account password. The purported Coinbase representative would also often cause a two-factor authentication code to be sent to the victim. The fake Coinbase representative would also trick the victim into providing that code to the conspirators. By tricking victims into providing the password reset link and/or the two-factor authentication code, the actors were able to access and subsequently gain control of the victims' Coinbase accounts.

5. After the conspirators gained unauthorized access to victims' Coinbase accounts, the actors, without the permission of the victims, transferred the victims' cryptocurrency holdings from the victims' wallets at Coinbase to cryptocurrency wallets in the fraudsters' control. TOMAR and his coconspirators controlled many cryptocurrency wallets which received hundreds of transactions of stolen cryptocurrency directly from victim accounts at Coinbase, totaling millions of dollars of cryptocurrency. Upon receipt of the stolen cryptocurrency, TOMAR quickly engaged in cryptocurrency transactions such as: (1) converting the funds into other forms of cryptocurrency, such as from Ethereum to Tether; and (2) moving the stolen funds amongst many wallets controlled by TOMAR and his coconspirators. Ultimately, the stolen cryptocurrency was converted into cash and distributed amongst TOMAR and his coconspirators.

6. TOMAR and his coconspirators stole millions of dollars' worth of cryptocurrency from victims located throughout the United States, including in the Western District of North

Carolina. An account at the cryptocurrency exchange Binance used by TOMAR and his coconspirators received over $9.5 million in stolen cryptocurrency pursuant to the conspiracy described herein. Thus, the conspiracy, to the extent to which Defendant was involved, caused victim losses of at least $9.5 million.

7. The fraud conspiracy involved 10 or more victims.

8. A substantial part of the fraudulent scheme was committed from outside the United States.

DENA J. KING
UNITED STATES ATTORNEY

MATTHEW WARREN
ASSISTANT UNITED STATES ATTORNEY

Defendant's Signature and Acknowledgment

I have read this Factual Basis, the Bill of Information, and the plea agreement in this case. I understand the Factual Basis, the Bill of Information, and the plea agreement. I hereby certify that I do not dispute this Factual Basis.

Chirag Tomar, Defendant

DATED: March 22, 2024

Defendant's Counsel's Signature and Acknowledgment

I have read this Factual Basis, the Bill of Information, and the plea agreement in this case, and have discussed them with the defendant. Based on those discussions, I am satisfied that the defendant understands the Factual Basis, the Bill of Information, and the plea agreement. I hereby certify that the defendant does not dispute this Factual Basis.

Russ Ferguson, Attorney for Defendant

DATED: March 22, 2024